UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA	:	
- v. -	:	S3 17 Cr. 548 (JMF)
JOSHUA ADAM SCHULTE,	:	
Defendant.	:	

GOVERNMENT'S OPPOSITION TO DEFENDANT'S MOTIONS TO DISMISS COUNTS THREE AND FOUR AND FOR INTERNET ACCESS

DAMIAN WILLIAMS
United States Attorney
Southern District of New York

David W. Denton, Jr.
Michael D. Lockard
Assistant United States Attorneys
- *Of Counsel* -

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page

Cases

Statutes

Rules

PRELIMINARY STATEMENT

The Government respectfully submits this memorandum in opposition to the defendant's *pro se* motions to dismiss counts three and four of the Third Superseding Indictment (the "Motion to Dismiss" or "MTD")[1] and for internet access while detained in the custody of the Bureau of Prisons ("BOP") (D.E. 557, the "Internet Access Motion" or "Int. Mot."). In the Motion to Dismiss, the defendant both (1) asks the Court resolve in his favor the jury question of whether particular information is in fact national defense information and (2) rehashes his previously-denied argument that one of his prison articles is protected by attorney-client privilege. The Internet Access Motion raises meritless claims that he has a right of access to the Internet in order to prepare for trial under the Fifth Amendment, and as a matter of free speech under the First Amendment. For the reasons discussed below, both motions should be denied.

BACKGROUND

As the Court is aware, the charges in this case stem from an investigation into WikiLeaks's disclosure of certain classified information stolen from the Central Intelligence Agency ("CIA"). Between March 7 and November 17, 2017, WikiLeaks made 26 separate disclosures of classified CIA information (together, the "Leaks"). The Leaks contained, among other things, highly sensitive CIA information including detailed descriptions of certain tools used by CIA operators (the "Stolen Information"). The Leaks' impact on the CIA's intelligence gathering activities and the national security of the United States was catastrophic.

The defendant was initially arrested on August 24, 2017, based on a criminal Complaint alleging child pornography crimes, and ordered detained. (D.E. 4). An indictment was returned on

---

[1] The Motion to Dismiss is dated October 8, 2021, and was filed with the Classified Information Security Officer ("CISO"). The Motion to Dismiss is currently undergoing a classification review and is not yet docketed.

September 6, 2017. (D.E. 6). At his arraignment, the defendant was released on conditions. (D.E. 8). On September 18, 2017, the Court entered a discovery protective order (D.E. 11 (the "Protective Order")) that prohibits disclosing protected materials outside the defense team. On August 16, 2018, the Court entered the Classified Information Protective Order that, inter alia, prohibits the defendant and defense counsel from disclosing classified information to anyone except the Court and government personnel holding the appropriate clearances and a need-to-know. (D.E. 61 at 5).

On December 14, 2017, following his arrest on state sexual assault charges in Virginia, the defendant's bail was revoked. (D.E. 22). The defendant moved to reinstate his bail, which the Court denied. (D.E. 26). The Court found that the defendant violated his conditions of release, including restrictions on internet access by having others access the internet on his behalf. (Jan. 8, 2018 Tr. at 16). The Court of Appeals affirmed the detention order. (D.E. 33).

On June 18, 2018, based on the information gathered as part of the investigation, the defendant was charged in a thirteen-count Indictment with espionage and other offenses related to the Leaks, as well as child pornography and copyright offenses for which the defendant previously was arrested. (D.E. 47 (First Superseding Indictment)).

Following the defendant's initial arrest, he engaged in a campaign to publicly promote false claims of having been framed by the Federal Bureau of Investigation ("FBI") and CIA. In May 2018, two newspapers published articles referencing search warrants produced in discovery pursuant to the Protective Order (the "Protected Search Warrants"). (Trial Tr. 2467-68, GX829). The Court held a hearing at which the Court reiterated the requirements of the Protective Order and confirmed that the defendant understood its terms. (*Id*. at 7-8).

In July 2018, the defendant's relatives posted to Facebook drafts of "articles" the defendant had written, but failed to post the versions that Schulte wanted publicized. (GX801, 806, 809). The

defendant's "articles" were part of his self-declared "information war" against the United States. (GX809). In approximately August 2018, the defendant and another inmate obtained access to contraband cellphones (the "Contraband Cellphones") (GX821, 5003), which the defendant used to create Facebook, Twitter, and email accounts, including encrypted and anonymized email accounts (the "Encrypted Accounts"). (GX809, 822, 1303-2). The defendant intended to publish his "articles" through these accounts, as well as purported statements by CIA and FBI employees claiming that the defendant was framed. (GX809). The defendant's draft posts included classified information about CIA cyber techniques and a particular CIA cyber tool called "Bartender." (*Id.*).

The defendant, pretending to be someone else, began communicating with one of the authors of the May 2018 articles in August 2018 using the Encrypted Accounts. (GX809, 1303-2, 1303-11). The defendant offered to provide the reporter with nonpublic information (*id*.), and in September 2018 emailed the reporter information from the Protected Search Warrants, including and an attempted refutation of statements in the supporting affidavit that included classified information. (GX1303-34). Before the defendant could disclose additional classified information, the FBI disrupted the defendant's plans. (Trial Tr. 2471, 2644).

Based on this conduct, on October 31, 2018, the grand jury returned a second superseding indictment charging him with one additional count of unlawfully disclosing and attempting to disclose classified information and one count of contempt of court. (D.E. 68 (Second Superseding Indictment)). The Attorney General also authorized Special Administrative Measures ("SAMs"), 28 C.F.R. Part 501. (D.E. 127 ("SAMs Order") at 3-4). Pursuant to the SAMs, the defendant is in a Special Housing Unit and has restricted and monitored communications. *Id.* at 4-5.

On February 2, 2020, trial began as to the eleven national security-related counts in the Second Superseding Indictment. On March 9, 2020, a jury found the defendant guilty of making

false statements to law enforcement, 18 U.S.C. § 1001, and contempt of court, 18 U.S.C. § 401(3). The jury did not reach a unanimous verdict on the remaining counts and the Court granted the defendant's motion for a mistrial as to those counts.

On June 8, 2020, a third superseding indictment was filed (D.E. 405 (Third Superseding Indictment)) containing nine counts based on the same conduct at issue during the February 2020 trial, namely, the defendant's theft and transmission of CIA information, his deletion of data on CIA computer systems while committing that theft, his obstruction of the resulting investigation, and his transmission and attempted transmission of classified information while detained. Count Three charges the defendant with unlawfully transmitting documents, writings, and notes relating to the national defense in or about September 2018, 18 U.S.C. §§ 793(e) and 2, based on his transmission of classified information to the reporter from the MCC. Count Four charges the defendant with attempting to unlawfully transmit documents, writings, and notes relating to the national defense between in or about July and October 2018, 18 U.S.C. §§ 793(e) and 2, based on his attempted transmission of classified information from the MCC.

DISCUSSION

I. The Motion to Dismiss Should Be Denied

A. Applicable Law

1. Standards for a Motion to Dismiss

"A party may raise by pretrial motion any defense, objection, or request that the court can determine without a trial on the merits." Fed. R. Crim. P. 12(b)(1). "In the ordinary course, in deciding a motion to dismiss, a court looks only to the face of the indictment." *United States v. Woodbine*, No. 02 CR. 150 (LAP), 2003 WL 1212972, at *1 (S.D.N.Y. Mar. 17, 2003). "[A]n indictment need do little more than to track the language of the statute charged and state the time and place (in approximate terms) of the alleged crime." *United States v. Alfonso*, 143 F.3d 772,

776 (2d Cir. 1998). "It is axiomatic that, in a criminal case, a defendant may not challenge a facially valid indictment prior to trial for insufficient evidence," *United States v. Gambino*, 809 F. Supp. 1061, 1079 (S.D.N.Y. 1992), and so "when a defense raises a factual dispute that is inextricably intertwined with a defendant's potential culpability, a judge cannot resolve that dispute on a Rule 12(b) motion," *United States v. Sampson*, 898 F.3d 270, 281 (2d Cir. 2018). To do so would "risk[] invading the inviolable function of the jury in our criminal justice system." *Id.* (internal quotation marks omitted).

The Second Circuit has acknowledged an "extraordinarily narrow" exception "to the rule that a court cannot test the sufficiency of the government's evidence on a Rule 12(b) motion," *id.* at 282, for rare cases where "the government has made what can fairly be described as a full proffer of the evidence it intends to present at trial to satisfy the jurisdictional element of the offense," *Alfonso*, 143 F.3d at 776-77. "[T]he government must make a 'detailed presentation of the entirety of the evidence' before a district court can dismiss an indictment on sufficiency grounds." *Sampson*, 898 F.3d at 282 (quoting *Alfonso*, 143 F.3d at 777). Outside of that narrow exception, "the appropriate time for a defendant's motion to dismiss based on insufficient evidence is ordinarily at the close of the government's case in chief when a defendant may make a Motion for a Judgment of Acquittal pursuant to Rule 29 of the Federal Rules of Criminal Procedure." *Woodbine*, 2003 WL 1212972, at *1.

2. As-Applied Challenges

"An 'as-applied challenge' . . . requires an analysis of the facts of a particular case to determine whether the application of a statute, even one constitutional on its face, deprived the individual to whom it was applied of a protected right." *Field Day, LLC v. Cty. of Suffolk*, 463 F.3d 167, 174 (2d Cir. 2006). "[I]t has never been deemed an abridgment of freedom of speech or press to make a course of conduct illegal merely because the conduct was in part initiated,

evidenced, or carried out by means of language, either spoken, written, or printed." *Giboney v. Empire Storage & Ice Co.*, 336 U.S. 490, 502 (1949). Thus, "[t]here are many federal provisions that forbid individuals from disclosing information they have lawfully obtained," including 18 U.S.C. § 793, and "[t]he validity of these provisions has long been assumed." *Boehner v. McDermott*, 484 F.3d 573, 578 (D.C. Cir. 2007). With respect to espionage prosecutions, "[t]here is no doubt the Government's interest in national security is compelling, and that '[m]easures to protect the secrecy of the Government's foreign intelligence operations plainly serve those interests.'" D.E. 284 at 5 (quoting *Haig v. Agee*, 453 U.S. 280, 307 (1981)). In evaluating an as-applied challenge to one who formerly was entrusted with national security information, "those who accept positions of trust involving a duty not to disclose information they lawfully acquire while performing their responsibilities have no First Amendment right to disclose that information." *Boehner*, 484 F.3d at 579. This is particularly true when the information was obtained unlawfully—it is "'beyond controversy that a recreant intelligence department employee who had abstracted from the government files secret intelligence information and had willfully transmitted or given it to one 'not entitled to receive it' as did the defendant in this case, is not entitled to invoke the First Amendment as a shield to immunize his act of thievery.'" D.E. 284 at 4 (quoting *United States v. Morison*, 844 F.2d 1057, 1069 (4th Cir. 1988)).

3. National Defense Information

The violations alleged in Counts Three and Four charge the defendant with transmitting and attempting to transmit "documents, writings, and notes relating to the national defense." 18 U.S.C. § 793(e). "[C]ourts have uniformly held . . . that 'national defense' is a 'generic concept of broad connotations, referring to the military and naval establishments and the related activities of national preparedness.'" *United States v. Abu-Jihaad*, 600 F. Supp. 2d 362, 385 (D. Conn. 2009) (quoting *Gorin v. United States*, 312 U.S. 19, 28 (1941)). "The question of the connection of the

information with national defense is a question of fact to be determined by the jury." *Gorin*, 312 U.S. at 32.

"Though the phrase 'information relating to the national defense' is quite broad, it is cabined" by the "judge-made" limitation that "the information must be 'closely held.'" *Abu-Jihaad*, 600 F. Supp. 2d at 386. In *Gorin*, the Supreme Court recognized that "[w]here there is no occasion for secrecy, as with reports relating to national defense, published by authority of Congress or the military departments, there can, of course, in all likelihood be no reasonable intent to give an advantage to a foreign government." 312 U.S. at 28. The Second Circuit expanded on this principle in *United States v. Heine*, holding that, since *Gorin* recognized that "it is obviously lawful to transmit any information about weapons and munitions of war which the services had themselves made public; . . . we can see no warrant for making a distinction between such information, and information which the services have never thought it necessary to withhold at all." 151 F.2d 813, 816 (2d Cir. 1945). Thus, if the Government has itself disclosed information, or has made no effort to guard the information against disclosure, it has not been "closely held." But courts have rejected the much broader proposition that "information that is available to the public can never be considered national defense information." *United States v. Squillacote*, 221 F.3d 542, 575 (4th Cir. 2000). It is axiomatic that "evidence of public disclosure does not deprive information of classified status where the classifying agency has demonstrated a reasonable basis for maintaining information as classified." D.E. 513 (Sept. 23, 2021 Order) at 3 (cleaned up, quoting *Wilson v. CIA*, 586 F.3d 171, 174 (2d Cir. 2009)). Courts "have unequivocally recognized that the fact that information resides in the public domain does not eliminate the possibility that further disclosures can cause harm to intelligence sources, methods and operations." *Fitzgibbon v. CIA*, 911 F.2d 755, 766 (D.C. Cir. 1990).

Thus, the question of whether information related to the national defense is "closely held" turns not merely on whether it has, in some form, been made public, but also *how* it became public. As the Fourth Circuit explained, "under *Gorin* and *Heine*, the central issue [of] the secrecy of the information . . . is determined by the government's actions," and the instructions to be given to a jury on this point should "properly focus[] the jury's attention on the actions of the government when determining whether the documents were related to the national defense." *Squillacote*, 221 F.3d at 577. Only "[w]here the information has been made public by the United States Government and is found in sources lawfully available to the general public, it is not 'closely held.' Similarly, where sources of information are lawfully available to the public *and the United States Government has made no effort to guard such information*, the information itself is not 'closely held.'" *Abu-Jihaad*, 600 F. Supp. 2d at 387 (emphasis added); *see also Squillacote*, 221 F.3d at 579 (approving instruction that "information made public by the government could not be considered national defense information, nor could publicly available information *that the government has never protected*") (emphasis added); D.E. 345 (jury charge) at 24 (same). The converse of these familiar propositions is also true: where material is made available to the public *unlawfully*, through illicit leaks to ones not entitled to receive it, and the Government *has* made efforts to guard the information, the jury can still conclude that it is national defense information.

B. Discussion

1. The Defendant's Motion to Dismiss Is Premature.

The defendant does not dispute that Counts Three and Four of the Third Superseding Indictment "track the language of the statute charged and state the time and place (in approximate terms) of the alleged crime." *Alfonso*, 143 F.3d at 776. Instead, the motion is largely premised on the defendant's contention that the information he is charged with disclosing and attempting to disclose in Counts Three and Four cannot qualify as national defense information because it had

already been publicly disclosed by WikiLeaks at the time that he included it in his communications with a reporter and attempted to make further disclosures online. (*See, e.g.*, MTD at 6). But "[t]he question of the connection of the information with national defense is a question of fact to be determined by the jury." *Gorin*, 312 U.S. at 32. The defendant's motion thus presents a paradigmatic example of a "factual dispute that is inextricably intertwined with a defendant's potential culpability" that the Second Circuit has held that "a judge cannot resolve . . . on a Rule 12(b) motion." *Sampson*, 898 F.3d at 281. The same is true of the defendant's assertion that he "provably took no substantial step" to transmit classified information from the MCC. (MTD at 26, 31). *See, e.g.*, *United States v. Helbrans*, No. 19 Cr. 497 (NSR), 2021 WL 2873800, at *14 (S.D.N.Y. July 8, 2021) ("[T]o the extent [the defendant] challenges the sufficiency or the quality of the Government's evidence that he performed (or aided and abetted) a substantial step, . . . that challenge is premature.").

At this pretrial stage, the defendant's motion therefore should be denied as premature since Counts Three and Four "contain[] the elements of the offense[s] charged and fairly inform[the] defendant of the charge[s] against which he must defend and . . . enable[] him to plead an acquittal or conviction in bar of future prosecutions for the same offense." *Hamling v. United States*, 418 U.S. 87, 117 (1974).[2]

---

[2] The evidence presented at the first trial does not constitute the sort of "full proffer of the evidence" that permits consideration of the sufficiency of that proof at the pretrial stage for the new counts charged in the currently operative indictment. *See Alfonso*, 143 F.3d at 776-77. On retrial, the Government expects to offer additional evidence related to the defendant's conduct at the MCC, and that conduct has been reframed as Counts Three and Four of the Third Superseding Indictment. But even if the Government's case at the first trial was considered such a proffer, the Court has already rejected the defendant's Rule 29 motion contesting the insufficiency of that proof. (*See* D.E. 581). Though the Court found that the evidence presented at trial was insufficient to show that the defendant's disclosure of information relating to one particular CIA network component included national defense information or that the defendant had reason to believe its

2. The Defendant's As-Applied Challenge Is Meritless.

The defendant's constitutional objection is explicitly framed as "as-applied challenges to counts three and four." (MTD at 1). The Court has already rejected the defendant's facial challenges to the constitutional validity of 18 U.S.C. § 793. (*See* D.E. 284). In that motion, however, the defendant "acknowledge[d] that the Espionage Act may constitutionally apply to him." (*Id.* at 8). Now, the defendant seeks to resurrect this challenge and contradict his earlier representations by asserting that, as applied to him, "the First Amendment clearly prohibits prosecution of citizens for discussing national news." (MTD at 1). But the defendant is not similarly situated to the public at large. "Mr. Schulte, as a government employee entrusted with sensitive information, had fair notice that his own alleged conduct was prohibited." (D.E. 169-3 at 19). Throughout his tenure at the CIA, Schulte signed non-disclosure agreements in which he acknowledged, among other things, "that by being granted access to classified information, special confidence and trust shall be placed in me by the United States Government," and that he

> will never divulge classified information to anyone unless: (a) I have officially verified that the recipient has been properly authorized by the United States Government to receive it; or (b) I have been given prior written notice of authorization from the United States Government Department or Agency . . . responsible for the classification of information or last granting me a security clearance that such disclosure is permitted.

---

disclosure could harm the United States, *id*. at 25 & n.11, Counts Three and Four of the Third Superseding Indictment charge a different offense under § 793(e): the disclosure of "documents, writings, and notes," rather than "information," which offense does not include as an element that the defendant had reason to believe the information could be used to the injury of the United States. *See* 18 U.S.C. § 793(e) (applying to disclosure of "any document, writing, . . . or note relating to the national defense, *or* information relating to the national defense which information the possessor has reason to believe could be used to the injury of the United States" (emphasis added)); *see also, e.g.*, *United States v. Drake*, 818 F. Supp. 2d 909, 916–17 (D. Md. 2011) ("[O]nly the second 'information' clause requires proof of the 'reason to believe' element."). As described above, the Government also intends to offer additional evidence at the retrial, further confirming that the resolution of what is squarely a question for the jury would be premature.

GX405 at 4. When a government employee "voluntarily assume[s] a duty of confidentiality, governmental restrictions on disclosure are not subject to the same stringent standards that would apply to efforts to impose restrictions on unwilling members of the public." *United States v. Aguilar*, 515 U.S. 593, 606 (1995); *see also United States v. Kim*, 808 F. Supp. 2d 44, 57 (D.D.C. 2011) ("By virtue of his security clearance, Defendant was entrusted with access to classified national security information and had a duty not to disclose that information. He cannot use the First Amendment to cloak his breach of that duty."); *cf. United States v. Kiriakou*, 898 F. Supp. 2d 921, 925 (E.D. Va. 2012) (there is "no question" that a "government employee trained in the classification system who could appreciate the significance of the information he allegedly disclosed . . . was on clear notice of the illegality of his alleged communications").

While it is true that "the CIA cannot prevent a former employee from publishing even properly classified information once the Agency itself has officially disclosed it," *Wilson*, 586 F.3d at 186, there is no dispute that the United States Government did not officially disclose the Stolen Information published within the Leaks. "[T]he law will not infer official disclosure of information classified by the CIA from . . . widespread public discussion of a classified matter." *Id.* In *Wilson*, the Second Circuit specifically rejected the same First Amendment claim that the defendant makes here, recognizing that the mere fact of public disclosure of classified information does not relieve a former intelligence officer of the security obligations the officer has undertaken:

> Ms. Wilson—like every other current and former Agency employee who has signed a Secrecy Agreement—"simply has no first amendment right to publish" the information here at issue, regardless of how "public" her past activities appear to have become. *Stillman v. CIA*, 319 F.3d at 548.
>
> The fact that others, not subject to such a secrecy obligation, are free to investigate Ms. Wilson's past and to compile and discuss all available information regarding her career . . . is not, as plaintiffs insist, an absurd or anomalous result. The law has long distinguished between "strangers," who "may republish previously published

> material," and former intelligence agents, who "are bound by formal agreements not to disclose [classified] information." *Alfred A. Knopf, Inc. v. Colby*, 509 F.2d [1362,] 1370 [(4th Cir. 1975)]. As noted, when Ms. Wilson elected to serve with the CIA, she accepted a life-long restriction on her ability to disclose classified and classifiable information. That Ms. Wilson's service may have been cut short by the failure of others to respect the classified status of her employment may well have warranted investigation. But these circumstances do not absolve Ms. Wilson of her own secrecy obligations.

Wilson, 586 F.3d at 196. Thus, the Court need not address the defendant's broad-based claims that the Government may not "charge private citizens with a crime for discussing information already on the internet." (MTD at 6). *This defendant* voluntarily accepted the restriction of his First Amendment rights through the numerous secrecy agreements that he signed with the CIA. "Courts have uniformly held that government employees who sign such nondisclosure agreements lack protection under the First Amendment," *Kim*, 808 F. Supp. 2d at 57, and *Wilson* expressly recognizes that public disclosure of the information at issue, when made unlawfully and in violation of classification procedures, does not relieve the defendant of those restrictions. Accordingly, the violations of 18 U.S.C. § 793 charged in Counts Three and Four do not "deprive[] the individual to whom [they are] applied of a protected right." *Field Day*, 463 F.3d at 167.

The defendant's argument also rests on the flawed contention that all of the information he disclosed and attempted to disclose is contained in the Leaks. *Cf. Wilson*, 586 F.3d at 186 ("Classified information that a party seeks to obtain or publish is deemed to have been officially disclosed only if it (1) is as specific as the information previously released, (2) matches the information previously disclosed, and (3) was made public through an official and documented disclosure." (cleaned up)). This contention is incorrect. For example, the defendant attempted to disclose that a "tool described in vendor report is in fact Bartender." GX-809 at 10 (reflecting CIPA § 6(c) substitution). The fact of Bartender's existence and its general description may have

been included in the Leaks, but the specific classified information the defendant attempted to disclose was not. The evidence at trial will show that other national defense information the defendant disclosed and attempted to disclose similarly was not included in the Leaks.

3. Unlawfully Leaked Information Still Qualifies as National Defense Information.

The Motion to Dismiss is also premised on two fundamentally incorrect understandings of what the Government must prove to show that the material at issue qualified as national defense information. The fact that information was unlawfully leaked to the public does not mean either (1) that it was not "closely held" by the Government or (2) that further disclosure would not be harmful to national security. As described above, these are factual questions that the Supreme Court has expressly committed to the jury's determination, and so the Court need not—and should not—address at this pretrial stage the defendant's assertions that the Government will not be able to carry its burden on these points. In any event, as discussed below, the premises underlying the defendant's argument are simply incorrect.

The charges against the defendant are not limited to his continued disclosure and attempted disclosure of information that he unlawfully transmitted and that WikiLeaks published in the Leaks. But the defendant's arguments are incorrect even to the extent they address information contained in the Leaks. First, in determining whether information is "closely held," "the central issue [of] the secrecy of the information . . . is determined by *the government's* actions," not those of third parties. *Squillacote*, 221 F.3d at 577 (emphasis added). The fact that information that the defendant stole was ultimately disseminated to the public does not give either Schulte or WikiLeaks the unilateral power to undermine "the government's actions" to keep that information secret. In a case such as this, where there is no contention that the Government itself released the Stolen Information, the jury's inquiry as to whether the information could be deemed not "closely

held" properly focuses on two issues: is the information "lawfully available to the general public," and has the United States "made no effort to guard such information." *Abu-Jihaad*, 600 F. Supp. 2d at 387. The Stolen Information in the Leaks satisfies neither.

It is beyond dispute that the Stolen Information contained in the Leaks was made public *unlawfully*. While the Government expects to prove that the defendant was responsible for the theft and disclosure of the Leaks, and is guilty of Counts One and Two of the Third Superseding Indictment, there is no question that, whoever was responsible for the theft, there was no lawful disclosure of the information. In addition, the Government made extensive "effort[s] to guard such information." The network from which the defendant took the Stolen Information was protected by restricting outside access to it; sequestering it from the internet; limiting access to approximately 200 individuals, each of whom possessed a Top Secret security clearance; requiring badges to enter the locked rooms secured by vault doors in which the network's terminals were stored; and protecting the CIA building in which the system was housed with armed guards and perimeter fencing. (*See* Trial Tr. 187, 194-96, 213, 552, 779, 900-01, 907). Moreover, the Stolen Information was—and remains today, with the exception of limited exhibits declassified for use at trial—classified. "Whether information is classified is relevant to whether information is considered closely held, which informs the jury's determination of whether a document constitutes national defense information." (D.E. 256 at 6). As the Court has frequently recognized, "evidence of public disclosure does not deprive information of classified status." (D.E. 513 at 3 (cleaned up, quoting *Wilson*, 586 F.3d at 174)). Although "the mere fact that information is classified does not"—standing alone—"mean that the information qualifies as national defense information" (D.E. 345 at 25), it is instructive as to the efforts made by the Government to guard the information. For example, in *United States v. Soblen*, 301 F.2d 236, 239 (2d Cir. 1962), the Second Circuit

recognized that "[t]he fact that the source of the information was classified as secret distinguishes this case from *United States v. Heine*," a case in which "no public authorities, naval, military or other, had ordered, or indeed suggested, that the manufacturers of airplanes—even including those made for the services—should withhold any facts," *Heine*, 151 F.2d at 815. It is thus entirely "consistent with the teachings of *Gorin* [and] *Heine*" that national defense information must be "closely held" for the Court to instruct the jury, as Judge Crotty did in the first trial of this matter, "that the information made public by the government could not be considered national defense information, nor could publicly available information that the government has never protected." *Squillacote*, 221 F.3d at 579. Where, as here, the Government *did* protect the Stolen Information, the fact that third parties—the defendant and WikiLeaks—subverted that protection does not warrant a conclusion that the information at issue was not "closely held."

Second, the fact that the Stolen Information was made public does not mean that further disclosures of it would not be harmful to the national defense. The defendant's principal contention is that, as a result of the Leaks, the CIA took certain corrective actions, and he infers that therefore there could be no harm from his additional disclosures. (*See, e.g.*, MTD at 12 ("[K]knowledge about Hickok in 2018 was deprecated, old news that was no longer accurate and could not possibly compromise any CIA network."); 28 ("[I]t was impossible for any statements about CIA tools or techniques developed pre-WikiLeaks to cause any harm."); 31 ("Bartender was no longer a tool used by the CIA."). But "the fact that information resides in the public domain does not eliminate the possibility that further disclosures can cause harm to intelligence sources, methods and operations." *Fitzgibbon*, 911 F.2d at 766. The defendant's contention ignores a variety of ways in which the disclosures and attempted disclosures charged in Counts Three and Four could harm national security. First and foremost, the fact that harm may have been mitigated does not mean

that harm has been eliminated. (*See, e.g.*, Trial Tr. 1514-15 (noting that even "after WikiLeaks posted CIA material," information about a classified CIA location was "still classified information, and there still is a security risk to people there then and throughout the future")). Second, the fact that the CIA decommissioned tools and networks in response to the Leaks was not public information at the time of the charged conduct—neither the defendant (who had by that time left the CIA) nor anyone else outside of the United States Government could have known at the time of the charged conduct that steps had been taken to address that harm. Third, the defendant relies solely on a forward-looking concept of harm—he ignores the significant harms that can occur from retrospective disclosures. The decommissioning of tools or shuttering of networks is, at most, relevant to whether the defendant's disclosures and attempted disclosures would have caused the specific harm of preventing future use of those tools or networks. It does not, however, prevent the harm that might occur, for example, from the identification of the use of a tool pre-dating the Leaks, the subsequent attribution of that tool to the CIA, and even the identification of the individuals responsible for deploying that tool. (*See, e.g.*, Trial Tr. 342 (noting that "attribution could lead to the capture of a CIA officer"); 1514 (noting that disclosure of "a classified program and capability . . . could pose kind of a national security risk to previous operations and future operations").[3]

---

[3] The defendant also argues that certain information cannot be considered national defense information because it was declassified in connection with his prosecution. (MTD at 31). That subsequent declassification does not retroactively immunize his crimes. Certain information (but not all of the leaked information) was declassified to implement the Court's rulings pursuant to CIPA and pursuant to Section 3.1(d) of Executive Order 13,526 (Dec. 29, 2009), which authorizes declassification when a responsible official finds that "the public interest in disclosure outweighs the damage to the national security that might reasonably be expected from disclosure." Declassification for trial in no way suggests that there was no harm to national security from the defendant's disclosures and attempted disclosures. Instead, declassification reflects the

Thus, while the question of whether the materials at issue constitute national defense information is properly committed to the jury, after hearing all the evidence, the defendant's substantive assertions are legally incorrect.

II. The Defendant Offers No Basis to Reconsider the Court's Prior Rulings that the Malware Article Is Not Privileged and Should Not Be Suppressed.

The defendant again repeats his claim that one article seized from him at the MCC is protected by the attorney-client privilege and should be suppressed. As the Court recognized in denying the defendant's most recent preceding motion to suppress material from the MCC as privileged during the November 8, 2021 conference in this matter, the parties extensively addressed with the Court the privilege status of portions of specific materials seized from the defendant at the MCC that the Government sought to introduce, and the Court concluded that three exhibits—GX 801, 806, and 809—were not privileged and were admitted into evidence as redacted. (*See* D.E. 288). The Government does not seek to offer additional material from the Malware Article, so the Court's prior rulings fully resolve this issue.

"Where a motion restates arguments already presented or attempts to advance new facts . . . the motion for reconsideration must be denied." *United States v. Alvarez-Estevez*, No. 13 Cr. 380 (JFK), 2014 WL 12681364, at *1 (S.D.N.Y. Nov. 6, 2014). In addition, Local Criminal Rule 49.1(d) requires a movant to submit a "memorandum setting forth concisely the matters or controlling decisions which counsel believes the Court has overlooked" within "fourteen (14) days after the Court's determination of the original motion." The untimeliness of a defendant's motion "is itself a sufficient basis for denial," although "courts retain the discretion to excuse an untimely filing." *United States v. Lisi*, No. 15 Cr. 457 (KPF), 2020 WL 1331955, at *1 (S.D.N.Y. Mar. 23,

---

determination that there is substantial public interest in a fair, open trial in which the defendant is held accountable for his acts of espionage.

2020). The defendant's motion, filed more than 20 months after the relevant portion of the document at issue was admitted into evidence following the Court's denial of his claim of privilege, provides no basis for reconsideration of the Court's prior rulings and is untimely. In any event, the motion is without merit, as reflected in the Court's prior rulings. Accordingly, the motion for reconsideration should be denied.

III. The Internet Access Motion Should Be Denied.

A. Procedural History

The Internet Access Motion is another in a string of challenges to the defendant's conditions of confinement. On May 10, 2019, the defendant (through counsel) filed a motion to vacate or modify the SAMs (D.E. 92), arguing that long-term solitary confinement constitutes torture (*id.* at 6-8), the SAMs fail to comply with the governing regulations (*id.* at 10-15), the SAMs are not rationally related to legitimate penological interests (*id*. at 10-15), and the SAMs' restrictions on Schulte's attorney-client communications and non-legal visits unconstitutionally burdened Schulte's First and Sixth Amendment rights (*id*. at 18-23).

Judge Crotty denied the motion, holding:

> The SAMs are undoubtedly restrictive, but generally they are reasonably necessary to avoid further disclosure of classified information. Despite escalating restrictions on Schulte's freedom prior to his isolation in 10 South, Schulte continued to flout Court orders and his bail conditions, protective order, BOP rules, and procedures for handling classified information. If the Government's allegations against Schulte are true, Schulte intended to engage in an information war which would involve leaking classified information to the news media. Restrictive measures needed to be placed on Schulte to prevent unauthorized disclosure of classified information.

(D.E. 127 at 8). The Court found appropriate minor modifications to provisions relating to defense-team communications with third parties (*id*. at 9-10) and contact with non-immediate family

members (*id*. at 11-12) to lessen the burden of the SAMs on the defendant's Sixth and First Amendment rights.

On June 24, 2021, Schulte's counsel filed his *pro se* motion to challenge the SAMs. (D.E. 474). Schulte argued that the SAMs violate the Fifth Amendment (*id*. at 2-3, 6-7) and separation-of-powers principles (*id*. at 7), and constitute cruel and unusual punishment (*id*. at 8-20). The Court denied the second SAMs motion, "repeat[ing] its 2019 holding that these measures, although hard, are '"reasonably related" to legitimate penological objectives' so long as Schulte is facing trial for substantial espionage charges, handling and reviewing sensitive classified material in discovery as he prepares his *pro se* defense, and continuing his troubling pattern of disrespect for the Court's protective orders and other directives regarding classified information." (D.E. 527 at 3) (quoting *United States v. El-Hage*, 213 F.3d 74, 81 (2d Cir. 2000)).

On August 3, 2021, the defendant filed a *pro se* motion seeking an order compelling the BOP and the Government to provide him with various accommodations and resources, including "24-7 access to his unclassified discovery" (*i.e.*, electrical outlets in his cell and a Government-provided CD/DVD burner), "24-7 access to a legal library such as the government utilizes[,]" and "24-7 access to a printer to print motions and court filings," arguing that the Fifth and Sixth Amendments provide him a right of "equal resources" to Government counsel and represented defendants. (D.E. 490). Judge Crotty denied the motion, observing that, when the defendant waived his right to counsel and elected to proceed *pro se*, he specifically acknowledged that:

> [A] professional attorney would not face the problems you're facing because you're incarcerated. And we can try to modify those conditions as we go along, but the fact of the matter is that you're always going to be at a deficit vis-à-vis retained or appointed counsel, who does not carry the burden of being incarcerated. And you are incarcerated. That causes certain problems in the preparation. If you want to represent yourself, that's fine. But you can't modify all of the conditions that are inhibiting you right now.

(D.E. 552 at 2). The Court held that, "[w]hile Schulte is certainly entitled to adequate means to represent himself, there are distinct limitations. Schulte is differently situated from other criminal defendants (represented and *pro se* alike) for several reasons, each of which were well-known to Schulte when he chose to discharge his competent and experienced counsel." *Id*. at 4. The Court further noted that "the parties, the CISO, and the Court have spent countless hours conferring and, in many instances, resorting to motion practice to chart a just and workable course through the web of confidentiality complexities and SAMs constraints inherent to these proceedings. As a result, Schulte has been afforded a suite of accommodations. . . . These accommodations resemble those that other courts have authorized for pro se criminal defendants subject to SAMs." *Id*. at 4-5. The Court directed that the parties meet and confer about any heightened trial preparation accommodations that may be possible after a trial date was set and as trial approaches. *Id*. at 6.[4]

BOP prohibits inmate internet access. BUREAU OF PRISONS, *Stay in Touch* (available at https://www.bop.gov/inmates/communications.jsp) ("Inmates' access to TRULINCS is controlled and inmates do not have access to the internet."); *see also* BUREAU OF PRISONS, Prog. Stmt. No. 4500.11, at 127 (Apr. 9, 2015) (available at https://www.bop.gov/policy/progstat/5265_013.pdf) ("Inmates do not have access to the Internet.").

The SAMs provide that the defendant may have access to publications and newspapers "determined not to facilitate criminal activity or be detrimental to national security; the security, good order, or discipline of the institution; or the protection of the public" (SAMs ¶ 8(a)) and to television and radio (*id*. ¶ 8(b)). The defendant also has access to legal research services through the BOP. (*See, e.g.*, D.E. 499 at 40-41) ("[T]he defendant has access to a LexisNexis legal research

[4] On November 5, 2021, the Court issued an order increasing the amount of time available to the defendant in the courthouse SCIF. (D.E. 575).

database provided by the [BOP] and available on a computer located in the defendant's unit . . . This database provides the defendant with access to case law and secondary legal materials.").

B. Applicable Law

While "[p]rison walls do not form a barrier separating prison inmates from the protections of the Constitution," *Turner v. Safley*, 482 U.S. 78, 83 (1987), "some rights are simply inconsistent with the status of a prisoner or with legitimate penological objectives of the corrections system," *Shaw v. Murphy*, 532 U.S. 223, 229 (2001). Where a defendant has been detained following a bail hearing, "the Government concededly may detain him to ensure his presence at trial and may subject him to the restrictions and conditions of the detention facility so long as those conditions and restrictions do not amount to punishment, or otherwise violate the Constitution." *Bell v. Wolfish*, 441 U.S. 520, 536-37 (1979). "Acknowledging the expertise of [prison] officials and that the judiciary is ill equipped to deal with the difficult and delicate problems of prison management, this Court has afforded considerable deference to the determinations of prison administrators who, in the interest of security, regulate the relations between prisoners and the outside world." *Thornburgh v. Abbott*, 490 U.S. 401, 407 (1989). The "test for evaluating prisoners' First Amendment challenges" is set forth in *Turner*. *Shaw*, 532 U.S. at 230. "[T]he regulation is valid if it is reasonably related to legitimate penological interests." *Id*. at 229. "First and foremost, there must be a valid, rational connection between the prison regulation and the legitimate and neutral government interest put forward to justify it." *Id*. (cleaned up). "[C]ourts should consider three other factors: the existence of alternative means of exercising the right available to inmates; the impact accommodation of the asserted constitutional right will have on guards and other inmates, and the allocation of prison resources generally; and the absence of ready alternatives available to the prison for achieving the governmental objectives." *Id*. at 229-30 (cleaned up). The Supreme Court has "sustained proscriptions of media interviews with individual inmates, prohibitions on

the activities of a prisoners' labor union, and restrictions on inmate-to-inmate correspondence." *Id*. at 229 (citations omitted).

C. Discussion

The defendant's argument that the Fifth and Sixth Amendments compel his right to access to the internet is based on the same flawed arguments he has presented in challenging other conditions of confinement: that he necessarily has a right to equal resources in all respects as Government counsel, unincarcerated defendants, and represented defendants. (Int. Mot. at 1 ("Mr. Schulte is entitled equal access."); 3 ("the defendant must also have equal access to the internet"); 4 (the government "must provide equal access to the internet to those detained pretrial just as it does to those released pending trial"); 4-5 (Schulte must have internet access because his former counsel had access).

The defendant cites no cases supporting this proposition, and there are none. "The essence of due process is the requirement that 'a person in jeopardy of serious loss (be given) notice of the case against him and opportunity to meet it.' All that is necessary is that the procedures be tailored, in light of the decision to be made, to 'the capacities and circumstances of those who are to be heard,' to insure that they are given a meaningful opportunity to present their case." *Mathews v. Eldridge*, 424 U.S. 319, 348-49 (1976). "The essential requirements of due process . . . are notice and an opportunity to respond." *Cleveland Bd. Educ. v. Loudermill*, 470 U.S. 532, 546 (1985). The Sixth Amendment provides a right to counsel, which the defendant has waived. "Apart from the right, in and of itself, to conduct one's own defense, a criminal defendant's decision to proceed *pro se* does not create new underlying protections." (D.E. 552 at 3). A defendant "has the right to legal help through appointed counsel, and when he declines that help, other alternative rights, like access to a law library, do not spring up." *United States v. Byrd*, 208 F.3d 592, 593 (7th Cir. 2000). Neither the Fifth nor Sixth Amendments provide the right Schulte asserts.

The Supreme Court has recognized, under the First Amendment, a "right of access" to the courts for incarcerated, *pro se* parties, to be free from interference with legal filings caused by a demonstrable inadequacy in a prison legal library. *Lewis v. Casey*, 518 U.S. 343, 351 (1996). Because there is no "freestanding right to a law library or legal assistance, an inmate cannot establish relevant actual injury simply by establishing that his prison's law library or legal assistance program is subpar in some theoretical sense." *Id*. There is also no right to compel the BOP "to enable the prisoner . . . to litigate effectively once in court." *Id*. at 354 (emphasis in original). Here, Schulte's contention that he cannot prepare his defense without internet access (Int. Mot. at 7-14) does not withstand scrutiny. He has "regular SCIF hours for classified discovery; access to legal research and unclassified discovery; special provisions expediting legal mail and correspondence from the Government; equipment, hardware, and other resources necessary to prepare his defense from the [BOP]; and standby counsel's assistance in briefing, arguing, corresponding, and filing." (D.E. 552 at 5; *see also* D.E. 575). Standby counsel is available to "assist[] the pro se defendant in overcoming routine procedural or evidentiary obstacles to the completion of some specific task." *McKaskle v. Wiggins*, 465 U.S. 168, 183 (1980). Even without internet access, he can (as he acknowledges) research secondary sources (Int. Mot. at 9), and he has written and filed numerous *pro se* motions and replies. In sum, none of the defendant's arguments show that he is not reasonably able to prepare for his defense. And to the extent that the defendant no longer has access to resources that his former counsel had, he was amply warned of that consequence before he knowingly, intelligently, and voluntarily waived his right to counsel. (D.E. 552 at 1-2).

The defendant's First Amendment challenge to his lack of internet access (Int. Mot. at 15-23) is a challenge to his conditions of confinement and not an issue relating to his constitutional

rights in defending this action, and properly brought as an independent action and not in a motion here. *See, e.g.*, D.E. 515 ("The Court agrees that a motion brought in the context of an ongoing criminal matter is not the proper venue to resolve correspondence issues pertaining to other actions.").[5] In a separate action, the court could evaluate the sufficiency of the defendant's allegations, the BOP would have an opportunity to respond, and, if necessary, the court could receive and evaluate evidence. The defendant's motion is not a proper vehicle for those matters.

Even on the merits, however, the defendant's First Amendment challenge should be readily denied. The BOP's prohibition on internet access by inmates is "reasonably related to legitimate penological interests." *Shaw*, 532 U.S. at 229. Not only does the BOP have a legitimate penological interest in being able to monitor, screen, and regulate inmates' access to media from outside the prison generally, *Abbott*, 490 U.S. at 415-19; *see also Duamutef v. Hollins*, 297 F.3d 108, 112 (2d Cir. 2002) ("the Supreme Court has upheld broad restrictions on prisoners' receipt of written materials"); but the BOP has a particularly strong penological interest in restricting Schulte's communications with individuals outside the prison. (D.E. 127 at 7-8; D.E. 527 at 3; D.E. 522 at 2-3). *See Duamutef*, 297 F.3d at 113 (finding mail screening "reasonably related to legitimate penological interests" where "plaintiff had an extensive disciplinary history involving prohibited organizational activities").

With respect to the other *Turner* factors, the defendant has "alternative means of exercising the right," *Shaw*, 532 U.S. at 230, consistent with the SAMs, including his ability to communicate with standby counsel, to communicate with family members, and to receive appropriate

[5] The defendant has numerous pending actions concerning allegations about his conditions of confinement. *See* 21-CV-4042 (JMF), 21-CV-4800 (JMF), 21-CV-5061 (JMF), 21-CV-5168 (JMF), 21-CV-5173 (JMF), 21-CV-5213 (JMF), 21-CV-5313 (JMF), 21-CV-5554 (JMF), 21-CV-5722 (JMF), 21-CV-5851 (JMF), 21-CV-5871 (JMF), 21-CV-6504 (JMF).

publications, radio, and television. "[I]t [is] sufficient if other means of expression . . . remain[] available," even if those other means are not similar to the prohibited conduct. *Abbott*, 490 U.S. at 417-18. The "impact accommodation of the asserted constitutional right will have on guards and other inmates," *Shaw*, 532 U.S. at 230, is self-evidently significant. It is not feasible to effectively monitor and screen the defendant's internet usage in advance. It can only be done after-the-fact, when the harm caused by inappropriate use of the internet has already occurred. And given the defendant's expertise in programming, malware, and computer networks, even after-the-fact monitoring would be insufficient to ensure his online activity was detected. *Compare Duamutef*, 297 F.3d at 113 ("Considering the limited resources of prison systems and the intense pressure to prevent security problems, we cannot expect more of corrections personnel in most circumstances."). Finally, there are no "ready alternatives available to the prison for achieving the governmental objectives," *id.*, that "fully accommodates" the prisoner's rights "at *de minimis* cost to valid penological interests." *Turner*, 482 U.S. at 90-91.

Accordingly, the defendant's motion for internet access should be denied.

CONCLUSION

For the foregoing reasons, the Government respectfully requests that the Court enter an order denying the Motion to Dismiss and the Motion for Internet Access.

Dated: November 12, 2021
New York, New York

DAMIAN WILLIAMS
United States Attorney

By: /s/
David W. Denton, Jr. / Michael D. Lockard
Assistant United States Attorneys
(212) 637-2744 / -2193

To: Joshua Adam Schulte (by hand, via MDC Legal Department)
Standby Counsel of Record (by ECF)